Title of the project :-

Data transmission in the Network Security

Overview :-

Data transmission in network communication is a critical aspect of modern connectivity, yet it presents various vulnerabilities that can compromise the security of transmitted information. Security is essential for maintaining the confidentiality, integrity, and availability of data from the vulnerabilites and mitigation.

Vulnerabilities:

1. Interception: Attackers can perform man-in-the-middle attacks, intercepting data and potentially altering it during transmission.
2. Exposure: Weakly encrypted or unencrypted data is susceptible to eavesdropping, allowing unauthorized parties to capture sensitive information.
3. Leakage: Improperly configured transmissions can unintentionally expose confidential data to unauthorized recipients.
4. Tampering: Hackers might modify transmitted data, leading to unauthorized changes and compromising data integrity.

List of teammates–

S.no	**name**	**collage**	**contact**
1	**Dr. S.K. Manju bargavi**	**Jain Deemed-to-be University**	**cloudbargavi@gmail.com**

List of Vulnerability Table –

S.no	Vulnerability Name	CWE – No
1	Man-in-the- Middle Attack	CWE-300
2.	Eavesdropping	CWE-200

3.	Data Leakage	CWE-532
4.	Session Hijacking	CWE-384
5.	Data Modification	CWE-613
6.	Replay Attack	CWE-294
7.	Insufficient Encryption	CWE-310
8.	Insecure Network Protocols	CWE-327
9.	Insecure Wireless Networks	CWE-330
10.	Insecure Channel	CWE-311

REPORT:-

Vulnerability Name: Man-in-the-Middle Attack

CWE Number: 300

OWASP Category: Insufficient Transport Layer Protection

Description: A Man-in-the-Middle (MitM) attack occurs when an attacker intercepts or alters the communication between two parties without their knowledge. The attacker secretly relays or alters the communication, potentially gaining access to sensitive information or injecting malicious content into the communication stream. This type of attack can compromise the confidentiality and integrity of the transmitted data.

Vulnerabilty Name : Eavesdropping
CWE Number: 200
OWASP Category: Insufficient Transport Layer Protection
Description: Eavesdropping refers to the unauthorized interception and monitoring of communication between two parties. Attackers capture data transmitted over a network without the knowledge of the sender or recipient. This can result in the exposure of sensitive information, such as passwords, personal details, or confidential data.
OWASP Category - Insufficient Transport Layer Protection:

The Insufficient Transport Layer Protection category in OWASP deals with vulnerabilities stemming from inadequate security measures at the transport layer. These vulnerabilities can include inadequate encryption, weak protocols, and misconfigurations that can be exploited by attackers to perform eavesdropping attacks and compromise the confidentiality of transmitted data.

To mitigate eavesdropping and related vulnerabilities, organizations should focus on implementing strong encryption protocols (such as TLS/SSL), ensuring secure configuration of transport layer security, and staying up-to-date with security best practices.

Vulnerability name: Data Leakage

- CWE Number: 532
- OWASP Category: Sensitive Data Exposure
- Description: Data leakage occurs when sensitive information is unintentionally exposed to unauthorized individuals or systems. This vulnerability can be caused by improper handling, weak security controls, or misconfigurations, leading to the potential exposure of sensitive data.

Session Hijacking:

- CWE Number: This vulnerability is commonly associated with CWE-384 (Session Fixation) and CWE-613 (Insufficient Session Expiration).
- OWASP Category: Broken Authentication
- Description: Session hijacking, also known as session fixation, involves an attacker taking control of a user's authenticated session. This can happen through various means, such as capturing session tokens, session IDs, or manipulating cookies. Once hijacked, the attacker gains unauthorized access to the user's account and privileges.

Vulnerability name :Data Modification

CWE Number: This vulnerability can be associated with various CWEs, including CWE-613 (Insufficient Session Expiration), CWE-348 (Use of Less Trusted Source), and others depending on the context.

OWASP Category: Broken Access Control

Description: Data modification refers to unauthorized alteration of data by attackers. This vulnerability occurs when an attacker gains the ability to change data without proper authorization. This can lead to data integrity issues, unauthorized changes, and potentially harmful consequences.

Vulnerability name: Replay Attack:

- CWE Number: This vulnerability is commonly associated with CWE-294 (Authentication Bypass by Capture-replay).
- OWASP Category: Broken Authentication
- Description: A replay attack involves the unauthorized capture and subsequent retransmission of valid data or requests. Attackers intercept and record legitimate data transmissions, then replay them at a later time to impersonate a legitimate user or gain unauthorized access.

Vulnerability name: Insufficient Encryption

- CWE Number: This vulnerability can be associated with various CWEs, including CWE-311 (Missing Encryption of Sensitive Data) and CWE-310 (Cryptographic Issues).
- OWASP Category: Insufficient Transport Layer Protection
- Description: Insufficient encryption refers to the inadequate protection of sensitive data during transmission or storage. Weak or improperly implemented encryption methods can lead to unauthorized access and data exposure.

Vulnerability name: Insufficient secure Protocols
CWE Number: 327
Description: This category focuses on situations where sensitive data is exposed due to inadequate security measures, including weak encryption. In the context of CWE-327, inadequate encryption strength could lead to sensitive data exposure if attackers can exploit the weaknesses in the encryption.

Vulnerability name: Insufficient wireless protocols
CWE Number :330
OWASP Category : Use of Insufficiently Random Values
Description : CWE-330 pertains to situations where an insecure random number generator (RNG) or insufficiently random values are used. This weakness can lead to vulnerabilities in various contexts, including encryption, authentication tokens, and cryptographic keys. While this CWE isn't specific to wireless networks, it could apply to issues related to weak or predictable keys used in securing wireless network communications.

Vulnerability name: Insecure channel
CWE Number: 311
OWASP Category : Missing Encryption of Sensitive Data
Description : CWE-311 refers to situations where sensitive information is transmitted over an insecure channel without proper encryption. This weakness can lead to data exposure, where attackers can intercept and read the transmitted data, potentially leading to compromise of sensitive information.

This category focuses on scenarios where sensitive data is exposed due to inadequate security measures, including situations where encryption is not used to protect data in transit. It addresses the risks associated with data being sent over insecure channels without proper encryption.

Stage 2

Overview :-

- Nessus is a widely used vulnerability scanning tool that helps in identifying security vulnerabilities, misconfigurations, and compliance issues in networks, systems, and applications.
- Developed by Tenable, Nessus offers comprehensive scanning capabilities and a vast vulnerability knowledge base to assist with risk assessment and remediation efforts.

Following operations are support from Nessus:

1. **Network Scanning**: Nessus performs active network scanning to discover and assess vulnerabilities in devices, servers, and network infrastructure. It sends various types of network packets to target hosts, attempting to identify open ports, running services, and potential security weaknesses. The goal of network scanning is to provide an overview of the security posture of the entire network, helping to identify areas that may be vulnerable to attacks.

2. **System Scanning**: Within network scanning, Nessus can perform detailed system-level scanning of discovered hosts. It attempts to identify security misconfigurations, known vulnerabilities in installed software, weak credentials, and other potential weaknesses that might expose the system to attacks.

3. **Web Application Scanning**: Nessus also offers web application scanning capabilities. It can analyze web applications and APIs for common security vulnerabilities like SQL injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), and more. By simulating attacks on web applications, Nessus helps identify potential security flaws that could be exploited by attackers.

4. **Credential-Based Scanning**: For certain types of scans, Nessus can perform credential-based scanning. This means that if provided with valid credentials, it can log in to target systems and conduct deeper checks. Credential-based scanning provides more accurate

results and allows Nessus to access information that may not be available through remote scans.

Target website — quillbot.com

Stage 3

Report

Title :-

Network Traffic Analysis -SOC/SIEM

Introduction

Network traffic analysis involves the examination of data packets transmitted over a network to understand and identify patterns, behaviors, anomalies, and potential security threats. By analyzing network traffic, organizations can detect various activities, such as unauthorized access attempts, data exfiltration, malware propagation, and more. Network traffic analysis can be performed using various techniques, including deep packet inspection, flow analysis, and behavior analysis.

SoC

A Security Operations Center (SOC) is a centralized unit within an organization responsible for monitoring, detecting, analyzing, and responding to security threats. Network traffic analysis is a fundamental activity performed by a SOC. Analysts within the SOC use tools and technologies to monitor network traffic, identify abnormal behavior, and respond to potential security incidents. SOC teams collaborate to investigate and mitigate threats, ensuring the organization's digital assets remain secure.

SOC – cycle

1. Detection:
    - Network Traffic Monitoring: The cycle begins with continuous monitoring of network traffic. SOC teams use various tools and technologies to capture and analyze network data, including packets, logs, and flow records.
    - Anomaly Detection: Network traffic analysis helps detect anomalies and deviations from normal patterns. Unusual traffic behavior, such as unexpected communication or unusual traffic volumes, can indicate potential security threats.
2. Alerting and Prioritization:
    - SIEM Correlation: The network traffic analysis results are often integrated into the Security Information and Event Management (SIEM) system. SIEM platforms

correlate data from network traffic analysis with other security data sources to identify potential threats.

- Alert Generation: Based on predefined correlation rules and behavioral analysis, the SIEM generates alerts for SOC analysts. These alerts prioritize potential incidents that require further investigation.

SIEM

A SIEM system is a technology solution that collects, correlates, and analyzes security-related information from various sources, including network devices, servers, applications, and security tools. SIEM platforms play a critical role in network traffic analysis within a SOC. They ingest logs and data from different sources, apply correlation rules to identify potential threats, and generate alerts for further investigation. SIEMs provide a holistic view of an organization's security posture by aggregating data from various sources and facilitating efficient incident response.

SIEM Cycle

Network traffic analysis is a crucial component of the Security Information and Event Management (SIEM) cycle. SIEM systems play a pivotal role in aggregating and analyzing data from various sources, including network traffic, to identify security incidents and trends. Here's how network traffic analysis fits into the SIEM cycle:

1. Data Collection:
    - Network Traffic Data: SIEM systems collect network traffic data, which includes logs, flow records, and packet captures. This data provides insights into communication patterns, user activities, and potential security threats.
2. Data Aggregation and Correlation:
    - Data Integration: The network traffic data is integrated into the SIEM platform alongside data from other sources, such as logs from servers, applications, and security devices.
    - Correlation Rules: SIEM systems apply correlation rules to analyze the combined data. These rules help identify relationships and patterns that might indicate security incidents.

MISP

A threat intelligence platform that allows users to exchange, store, and correlate threat intelligence, financial fraud, vulnerability, and counter-terrorism information as well as indicators of compromise from targeted attacks. Find out how MISP is currently being used by various organisations. The IoCs and information are used to not only store, share, and collaborate on malware research and cyber security indicators, but also to identify and stop attacks on ICT infrastructures, businesses, or individuals.

College network information

- In my college used in network filtering for prevention technique
- How you think you deploy soc in your college
    - Its more secure and useful for all information about college.

Threat intelligence

- Patterns observed in network traffic analysis contribute to threat intelligence, helping organizations stay informed about emerging threats.
- Incident response

  SOC analysts use the information from network traffic analysis to investigate alerts. They analyze suspicious network activities and attempt to understand the nature of the incident.

Qradar & understanding about tool

- Qradar is a more powerful tool for SOC and SIEM.
- In Network traffic analysis project required for Qradar tool. It may provides the following process,
    - Anomaly Detection
    - Real-time Threat Detection
    - Incident Investigation
    - Advanced Threat Intelligence
    - Compilance Monitoring and Reporting etc.,

Conclusion :-

- Stage 1 :- Security process is more important for deploying the web application.
- Stage 2 :- Analysis the nessus tool for hacking.
- Stage 3 :- Specific application like prevention and detection for SOC/SIEM/Qradar tool

Future Scope :-

- Stage 1 :- More protective pattern for web application
- Stage 2 :- Nessus is major role for analysing and hacking in future
- Stage 3 :- In future, all kinds of operations (Security) will perform through SOC/SIEM.

—--------THE END —-----------------------